

1 **CLAIMS**

2 What is claimed is:

3 1. A method comprising:  
4 establishing at least one cryptography service parameter threshold;  
5 selectively detecting a request for at least one cryptography service; and  
6 selectively performing at least one correctness detection action based on  
7 said requested cryptography service and said at least one cryptography service  
8 parameter threshold.

9  
10 2. The method as recited in Claim 1, wherein establishing said at least  
11 one cryptography service parameter threshold includes at least identifying  
12 unacceptable cryptography algorithms.

13  
14 3. The method as recited in Claim 1, wherein establishing said at least  
15 one cryptography service parameter threshold includes at least identifying  
16 acceptable cryptography algorithms.

17  
18 4. The method as recited in Claim 1, wherein establishing said at least  
19 one cryptography service parameter threshold includes at least identifying at least  
20 one unacceptable cryptography key size parameter.

21  
22 5. The method as recited in Claim 1, wherein establishing said at least  
23 one cryptography service parameter threshold includes at least identifying at least  
24 one acceptable cryptography key size parameter.  
25

1           6.     The method as recited in Claim 1, wherein establishing said at least  
2 one cryptography service parameter threshold includes establishing a plurality of  
3 correctness categories, wherein each at least one of said plurality of correctness  
4 categories includes at least one cryptography algorithm identifier.

5  
6           7.     The method as recited in Claim 6, wherein said plurality of  
7 correctness categories includes at least one correctness category selected from a  
8 group of correctness categories comprising authorized algorithms, unauthorized  
9 algorithms, weak algorithms, and strong algorithms.

10  
11           8.     The method as recited in Claim 1, wherein establishing said at least  
12 one cryptography service parameter threshold includes at least identifying at least  
13 one acceptable seed size parameter.

14  
15           9.     The method as recited in Claim 1, wherein establishing said at least  
16 one cryptography service parameter threshold includes at least identifying at least  
17 one unacceptable seed size parameter.

18  
19           10.    The method as recited in Claim 1, wherein selectively detecting said  
20 request for at least one cryptography service includes monitoring at least one  
21 process selected from a group of processes comprising an application, an operating  
22 system, a cryptography system service, and another process calling into the  
23 cryptography application programming interfaces.

1           11. The method as recited in Claim 1, wherein selectively performing at  
2 least one correctness detection action based on said requested cryptography  
3 service and said at least one cryptography service parameter threshold includes  
4 determining if a cryptographic key associated with said requested cryptography  
5 service is suitable for use based on said at least one cryptography service  
6 parameter threshold.

7  
8           12. The method as recited in Claim 11, wherein determining if said  
9 cryptographic key associated with said requested cryptography service is suitable  
10 for use based on said at least one cryptography service parameter threshold  
11 includes comparing a size of said cryptographic key with said at least one  
12 cryptography service parameter threshold.

13  
14           13. The method as recited in Claim 1, wherein selectively performing at  
15 least one correctness detection action based on said requested cryptography  
16 service and said at least one cryptography service parameter threshold includes  
17 determining if a cryptographic algorithm associated with said requested  
18 cryptography service is suitable for use based on said at least one cryptography  
19 service parameter threshold.

20  
21           14. The method as recited in Claim 13, wherein determining if said  
22 cryptographic algorithm associated with said requested cryptography service is  
23 suitable for use based on said at least one cryptography service parameter  
24 threshold further includes comparing a cryptography algorithm identifier with said  
25 at least one cryptography service parameter threshold.

1  
2        15.    The method as recited in Claim 1, wherein selectively performing at  
3 least one correctness detection action based on said requested cryptography  
4 service and said at least one cryptography service parameter threshold includes  
5 performing at least one action selected from a group of actions comprising  
6 interrupting at least one process, stopping at least one process, starting at least one  
7 process, displaying alert information, logging alert information, suggesting at least  
8 one alternative cryptography service, outputting alert messages, causing alteration  
9 of a graphical user interface, and forcing use of at least one other cryptography  
10 service.

11  
12        16.    A computer readable medium having computer-implementable  
13 instructions for causing one or more processing units to perform acts comprising:  
14        selectively detecting a request for at least one cryptography service; and  
15        selectively performing at least one correctness detection action based on  
16 said requested cryptography service if said requested cryptography service does  
17 not satisfy at least one cryptography service parameter threshold.

18  
19        17.    The computer readable medium as recited in Claim 16, further  
20 comprising:  
21        establishing said at least one cryptography service parameter threshold.

1           18.    The computer readable medium as recited in Claim 17, wherein  
2 establishing said at least one cryptography service parameter threshold includes at  
3 least one of the following acts:

4               identifying unacceptable cryptography algorithms; and  
5               identifying acceptable cryptography algorithms.

6  
7           19.    The computer readable medium as recited in Claim 17, wherein  
8 establishing said at least one cryptography service parameter threshold includes at  
9 least one of the following acts:

10              identifying at least one unacceptable cryptography key size parameter; and  
11              identifying at least one acceptable cryptography key size parameter.

12  
13           20.    The computer readable medium as recited in Claim 17, wherein  
14 establishing said at least one cryptography service parameter threshold includes  
15 establishing a plurality of correctness categories, wherein each at least one of said  
16 plurality of correctness categories includes at least one cryptography algorithm  
17 identifier.

18  
19           21.    The computer readable medium as recited in Claim 20, wherein said  
20 plurality of correctness categories includes at least one correctness category  
21 selected from a group of correctness categories comprising authorized algorithms,  
22 unauthorized algorithms, weak algorithms, and strong algorithms.

1           22. The computer readable medium as recited in Claim 17, wherein  
2 establishing said at least one cryptography service parameter threshold includes at  
3 least one of the following acts:

4           identifying at least one acceptable seed size parameter; and  
5           identifying at least one unacceptable seed size parameter.  
6

7           23. The computer readable medium as recited in Claim 16, wherein  
8 selectively detecting said request for at least one cryptography service includes  
9 monitoring at least one process selected from a group of processes comprising an  
10 application, an operating system, a cryptography algorithm, and a cryptography  
11 application programming interface.  
12

13           24. The computer readable medium as recited in Claim 16, wherein  
14 selectively performing said at least one correctness detection action based on said  
15 requested cryptography service if said requested cryptography service does not  
16 satisfy said at least one cryptography service parameter threshold includes  
17 determining if a cryptographic key associated with said requested cryptography  
18 service is suitable for use based on said at least one cryptography service  
19 parameter threshold.  
20

21           25. The computer readable medium as recited in Claim 24, wherein  
22 determining if said cryptographic key associated with said requested cryptography  
23 service is suitable for use based on said at least one cryptography service  
24 parameter threshold includes comparing a size of said cryptographic key with said  
25 at least one cryptography service parameter threshold.

1  
2        26.    The computer readable medium as recited in Claim 16, wherein  
3 selectively performing said at least one correctness detection action based on said  
4 requested cryptography service if said requested cryptography service does not  
5 satisfy said at least one cryptography service parameter threshold includes  
6 determining if a cryptographic algorithm associated with said requested  
7 cryptography service is suitable for use based on said at least one cryptography  
8 service parameter threshold.

9  
10       27.    The computer readable medium as recited in Claim 26, wherein  
11 determining if said cryptographic algorithm associated with said requested  
12 cryptography service is suitable for use based on said at least one cryptography  
13 service parameter threshold further includes comparing a cryptography algorithm  
14 identifier with said at least one cryptography service parameter threshold.

15  
16       28.    The computer readable medium as recited in Claim 16, wherein  
17 selectively performing said at least one correctness detection action based on said  
18 requested cryptography service if said requested cryptography service does not  
19 satisfy said at least one cryptography service parameter threshold includes  
20 performing at least one action selected from a group of actions comprising  
21 interrupting at least one process, stopping at least one process, starting at least one  
22 process, displaying alert information, logging alert information, suggesting at least  
23 one alternative cryptography service, outputting alert messages, causing alteration  
24 of a graphical user interface, and forcing use of at least one other cryptography  
25 service.

1  
2 29. An apparatus comprising:

3 cryptography correctness detection logic configured to selectively detect a  
4 request for at least one cryptography service, and selectively least one correctness  
5 detection action to be performed based on said requested cryptography service if  
6 said requested cryptography service does not satisfy at least one cryptography  
7 service parameter threshold.  
8

9 30. The apparatus as recited in Claim 29, further comprising:

10 memory operatively coupled to said cryptography correctness detection  
11 logic; and

12 wherein said cryptography correctness detection logic is further configured  
13 to maintain said at least one cryptography service parameter threshold in said  
14 memory.  
15

16 31. The apparatus as recited in Claim 30, wherein said cryptography  
17 correctness detection logic is further configured to identify at least one of the  
18 following: at least one unacceptable cryptography algorithm, and at least one  
19 acceptable cryptography algorithm.  
20

21 32. The apparatus as recited in Claim 30, wherein said cryptography  
22 correctness detection logic is further configured to identify at least one of the  
23 following: at least one unacceptable cryptography key size parameter; and at least  
24 one acceptable cryptography key size parameter.  
25



1           33. The apparatus as recited in Claim 30, wherein said cryptography  
2 correctness detection logic is further configured to establish a plurality of  
3 correctness categories in said memory, wherein each at least one of said plurality  
4 of correctness categories includes at least one cryptography algorithm identifier.

5  
6           34. The apparatus as recited in Claim 30, wherein said cryptography  
7 correctness detection logic is further configured to identify at least one of the  
8 following:

9           at least one acceptable seed size parameter; and

10          at least one unacceptable seed size parameter.

11  
12          35. The apparatus as recited in Claim 29, wherein said cryptography  
13 correctness detection logic is further configured to monitor at least one process  
14 selected from a group of processes comprising an application, an operating  
15 system, a cryptography algorithm, and a cryptography application programming  
16 interface.

17  
18          36. The apparatus as recited in Claim 29, wherein said cryptography  
19 correctness detection logic is further configured to determine if a cryptographic  
20 key associated with said requested cryptography service is suitable for use based  
21 on said at least one cryptography service parameter threshold.

22  
23          37. The apparatus as recited in Claim 36, wherein said cryptography  
24 correctness detection logic is further configured to compare a size of said  
25 cryptographic key with said at least one cryptography service parameter threshold.

1  
2 38. The apparatus as recited in Claim 29, wherein said cryptography  
3 correctness detection logic is further configured to determine if a cryptographic  
4 algorithm associated with said requested cryptography service is suitable for use  
5 based on said at least one cryptography service parameter threshold.

6  
7 39. The apparatus as recited in Claim 38, wherein said cryptography  
8 correctness detection logic is further configured to compare a cryptography  
9 algorithm identifier with said at least one cryptography service parameter  
10 threshold.

11  
12 40. The apparatus as recited in Claim 29, wherein said cryptography  
13 correctness detection logic is further configured to cause at least one action  
14 selected from a group of actions comprising interrupting at least one process,  
15 stopping at least one process, starting at least one process, displaying alert  
16 information, logging alert information, suggesting at least one alternative  
17 cryptography service, outputting alert messages, causing alteration of a graphical  
18 user interface, and forcing use of at least one other cryptography service, to be  
19 performed